



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/710,541	11/09/2000	Christopher Paul Carroll	99-956	5815
32127	7590	09/30/2004	EXAMINER	
VERIZON CORPORATE SERVICES GROUP INC. C/O CHRISTIAN R. ANDERSEN 600 HIDDEN RIDGE DRIVE MAILCODE HQEO3H14 IRVING, TX 75038				NOBAHAR, ABDULHAKIM
ART UNIT		PAPER NUMBER		
		2132		
DATE MAILED: 09/30/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/710,541	CARROLL, CHRISTOPHER PAUL
	Examiner Abdulhakim Nobahar	Art Unit 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on ____.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-32 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-32 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 1 June 2001.

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
5) Notice of Informal Patent Application (PTO-152)
6) Other: ____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 21 recites the limitation "MODE field" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 32 recites the limitation " using 3GPP (Third Generation Project Partners) AKA (authentication and key agreement) " in line 11-13. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 19-26, 30 and 31 are rejected under 35 U.S.C. 102(e) as being anticipated by Aura (6,711,400 B1).

Aura discloses an authentication method for a telecommunication system that a mobile subscriber is authenticated to both visiting and home networks and vice versa (see, for example, abstract), i.e., the authenticity of the subscriber's identity is verified by the networks and the subscriber checks the authenticity of the networks' identities.

Claim 19

Aura discloses:

determining at the home environment network a cryptographic primitive offered by the service network (see, for example, Fig. 3, where the home network at stage 302 uses the primitive TA11 for calculation of KS and the service network BS uses primitive TA12 at stage 312 to calculate DCK1 which also calculated by MS at stage 323 using TA12. The calculation of DCK1 at MS is dependent upon the value KS. This implies that the home network is aware of the primitive used at the BS and based on this knowledge the home network transmits the required authentication vector to the visiting network to be used by a specific primitive which corresponds to the recited determining at the home environment network a cryptographic primitive...); and based on the determined cryptographic primitive, transmitting to the service network at least one vector of authentication information corresponding to a particular station (see, for example, Fig. 3, where the home network transmit the vector RS at stage 303 to the BS that is used by the MS at stage 321).

Claim 20

Aura discloses:

receiving identification of the cryptographic primitive from the service network
(see, for example, Fig. 4, where RAND2 received by MS at stage 407 which is
generated by the home network using a hash function at stage 404).

Claim 21

Aura discloses:

identification comprises a value of a MODE field (see, for example, Fig. 4, where
SRES1 which is the product of a hash value that represents a value corresponding to
the recited MODE field).

Claim 22

Aura discloses:

the vector authentication information comprises an indication of an authentication
vector sequence number maintained by the home environment network. (see, for
example, Fig. 4, where RAND2, SRES1, SRES2' and Kc are the vector of
authentication information received by the visited network from the home network and
these information are based on Ki which represents the encryption key for the ith mobile
station that corresponds to the ith position of a vector in the sequence a I's values of
vector information)

Claim 23

Aura discloses:

The vector of authentication information comprises a challenge and an expected response (see, for example, Fig. 4, where the challenge RAND2 at stage 407 is received by MS and the SRES2 is the expected response).

Claim 24

Aura discloses:

storing different sets of cryptographic information for the different respective service networks (see, for example, Fig. 3, where the computed DCK at stage 327 maintained by MS is used in conjunction with a particular visiting network BS); selecting a set of cryptographic information for one of the service networks; and using the selected set of cryptographic information to communicate with the service network (see, for example, Fig. 3, where the computed DCK at stage 327 by MS is selected for encrypting the communication with a particular visiting network BS).

Claim 25

Aura discloses:

the sets of cryptographic information comprise a key shared by the station and the service network (see, for example, Fig. 3, where the cryptographic key DCK is used by both MS and the visiting network for communicating with each other).

Claim 26

Aura discloses:

computing the key shared by the station and the service network based on information received from the service network (see, for example, Fig. 3, where at stage 327 the cryptographic key DCK is computed based on the DCK1 and DCK2 that are in turn computed based on KS and KS'. The KS and KS' are calculated based on RS received from the service network. Thus, DCK is based on the RS).

Claim 30

Aura discloses:

using the selected set of cryptographic information comprises using the selected set cryptographic information to authenticate the service network (see, for example, Fig. 4, where the cryptographic key Ki is selected by the MS to calculate SRES1' in order to authenticate the visiting network at stage 408).

Claim 31

Aura discloses:

using the selected set cryptographic information comprises using the selected set of cryptographic information in encrypting communication between the station and the service network (see, for example, Fig. 4, where the cryptographic key Kc is selected for encrypting communication between the station and the service network).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-18 and 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aura (6,711,400 B1) in view of Marshall et al (4,888,800; hereinafter Marshall).

Aura discloses an authentication method for a telecommunication system that a mobile subscriber is authenticated to both visiting and home networks and vice versa (see, for example, abstract), i.e., the authenticity of the subscriber's identity is verified by the networks and the subscriber checks the authenticity of the networks' identities.

Marshall discloses a secure communication system that enables two terminals to transmit secure messages to each other. One of the terminals requests a key distribution center to provide encryption keys to both terminals, after a link is established between the two (see, for example, abstract and col. 1, lines 33-49).

Claim 1

Aura discloses:

storing a key at the service network (see, for example, col. 3, lines 1-4; col. 7, lines 7-12, where the visited network VPLMN corresponds to the recited service network);

transmitting information to the station from the service network that enables the station to compute the key stored at the service network (see, for example, col. 7, lines 13-25);

receiving a request for service at the service network from the station (see, for example, col. 6, lines 16-21);

Aura, however, does not expressly disclose:

adjusting a value corresponding to key usage; and

transmitting information corresponding to the value to the station.

Marshall discloses the use of a counter in association with the usage of an encryption key by a terminal (corresponding to the recited mobile station). When the counter reaches a predetermined value a new key is transported to the terminal that corresponds to the recited transmitting information corresponding to the value to the station (see, for example, abstract; col. 7, lines 15-25).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement a key usage counter as taught in Marshall in the method of Aura because it would provide a means for updating the encryption key (col.

2, lines 10-20) and that in turn would prevent an outsider to eventually gain access to the encryption keys (col. 6, lines 35-40).

Claim 2

Aura discloses:

receiving a vector of authentication information from the home environment network of the station, the vector including an indication of the vector's position in a sequence of vectors (see, for example, Fig. 4, where RAND2, SRES1, SRES2' and Kc are the vector of authentication information received by the visited network from the home network and these information are based on Ki which represents the encryption key for the ith mobile station that corresponds to the ith position of a vector in the sequence a I's values of vector information); and

transmitting information to the station that enables the station to compute the key stored at the service network comprises transmitting portions of the received vector of authentication information (see, for example, Fig. 4, where RAND2 and SRES1 are a portion of the received vector of authentication information and transmitted to the ith mobile station to calculate Kc stored also in the visited network).

Claim 3

Aura discloses:

the received vector of authentication information comprises the key stored by the service network (see, for example, Fig. 4, where the key Kc is received and stored by the visited network).

Claim 4

Aura discloses:

computing at the service network the key stored by the service network based on information included in the received vector (see, for example, Fig. 3, where the key DKC is computed at the visiting network using DCK 1 and DCK2 that in turn are calculated using the information KS and KS' received from the home network, i.e., the vector).

Claim 5

Marshall discloses:

adjusting a value indicating use of the key comprises incrementing a sequence number corresponding to a number of times the key has been used (see, for example, col. 7, lines 15-25).

Claim 6

Marshall discloses:

the value comprises a TSQN (Temporary Sequence Number) (see, for example, col. 7, lines 21-25, where setting the value of the counter to zero corresponds to a temporary sequence number).

Claim 7

Aura discloses:

the station comprises a cellular phone; and

the service network and home environment networks comprise cellular networks
(see, for example, col. 1, line 49-col. 2, line 3 and Fig. 1).

Claim 8

Aura discloses:

using the key to compute a cipher key for encrypting communication between the service network and the station (see, for example, Fig. 3, where the key DCK is calculated for encrypting communication between the visited network and the mobile station at stages 327 and 315).

Claim 9

Aura discloses:

negotiating use of a cryptographic primitive between the service network and the home environment network (see, for example, Fig. 3, where the home network at stage 302 uses the primitive TA11 for calculation of KS and the service network BS uses primitive TA12 at stage 312 to calculate DCK1 which also calculated by MS at stage 323 using TA12. The calculation of DCK1 at MS is dependent upon the value KS. This implies that the home network is aware of the primitives used at the BS and based on this knowledge the home network transmits the required authentication vector to the visiting network to be used by a specific primitive which corresponds to the recited negotiating use of a cryptographic primitive...).

Claim 10

Aura discloses:

transmitting a challenge to the station (see, for example, Fig. 4, where the challenge RAND2 at stage 406 is sent to the MS);
receiving a challenge response from the station (see, for example, Fig. 4, where the SRES2 at stage 409 is received); and
comparing the received challenge response with an expected response (see, for example, Fig. 4, stage 409).

Claim 11

Aura discloses:

computing the key stored by the service network at the station (see, for example, Fig. 4, stage 407, the key Kc is calculated and also stored at the VPLMN).

Aura, however, does not expressly disclose:

receiving the information indicating the value corresponding to key usage at the station; and

comparing the received value with a value corresponding to key usage maintained by the station.

Marshall discloses the use of a counter in association with the usage of an encryption key by a terminal (corresponding to the recited mobile station). When the counter reaches a predetermined value (corresponding to the recited comparing the received value with another value for key usage) a new key is transported to the

terminal that corresponds to the recited transmitting information corresponding to the value to the station (see, for example, abstract; col. 7, lines 15-25).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement a key usage counter as taught in Marshall in the method of Aura because it would provide a means for updating the encryption key (col. 2, lines 10-20) and that in turn would prevent an outsider to eventually gain access to the encryption keys (col. 6, lines 35-40).

Claim 12

Aura discloses:

A method for use in authenticating a service network to a station, the station having a home environment network, the method comprising:

receiving information at the station from the service network (see, for example, Fig. 4, RAND2 and SRES1 at stage 407);

computing a key based on the information received at the station from the service network, the computed key also being stored by the service network (see, for example, Fig. 4, Kc at stage 407);

Aura, however, does not expressly disclose:

maintaining an indicator of key usage at the station;

receiving at the station an indicator of key usage maintained by the service network; and

comparing the key usage indicator maintained by the service network with the key usage indicator maintained by the station.

Marshall discloses the use of counters in association with the usage of encryption keys by both terminals (corresponding to the recited mobile station and service network). When the counters reach a predetermined value (corresponding to the recited comparing the indicator of the service network with the indicator of the mobile station) a new key is transported to the terminal that corresponds to the recited transmitting information corresponding to the value to the station (see, for example, abstract; col. 7, lines 15-25).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement a key usage counter as taught in Marshall in the method of Aura because it would provide a means for updating the encryption key (col. 2, lines 10-20) and that in turn would prevent an outsider to eventually gain access to the encryption keys (col. 6, lines 35-40).

Claim 13

Aura discloses:

maintaining an authentication vector sequence number at the station (see, for example, col. 8, line 65-col. 9, line 2);

receiving at the station from the service network an indication of an authentication vector sequence number maintained by the home environment network

(see, for example, Fig. 4, where SRES1 is received by the MS from VPLMN at stage 407 which is kept at HLR/AUC; and

comparing the authentication vector sequence number maintained by the home environment network with the received authentication vector sequence number maintained by the station (see, for example, Fig. 4, where SRES1 maintained by the home network is compared with SRES1' maintained by the MS at stage 408).

Claim 14

Aura discloses:

receiving from the service network identification of a cryptographic primitive (see, for example, Fig. 4, where RAND2 received by MS at stage 407 which is generated by the home network using a hash function at stage 404).

Claim 15

Aura discloses:

the station comprises a cellular phone; and

the service network and home environment networks comprise cellular networks (see, for example, col. 1, line 49-col. 2, line 3 and Fig. 1).

Claim 16

Aura discloses:

using the key to compute a cipher key for encrypting communication between the service network and the station (see, for example, Fig. 3, where the key DCK is calculated for encrypting communication between the visited network and the mobile station at stages 327 and 315).

Claim 17

Aura discloses:

receiving a challenge from the service network (see, for example, Fig. 4, where the challenge RAND2 at stage 407 is received by MS);

determining a challenge response (see, for example, Fig. 4, where at stage 407 SRES2 is computed); and

transmitting the challenge response to the service network (see, for example, Fig. 4, where SRES2 is transmitted to VPLMN at stage 409).

Claim 18

Marshall discloses the use of a counter in association with the usage of an encryption key by a terminal (corresponding to the recited mobile station) (see, for example, abstract; col. 7, lines 15-25).

Claim 27

Aura does not expressly disclose:

the sets of cryptographic information comprise an indicator of usage of the key

Marshall discloses the use of counters indicating the usage of encryption keys by both terminals (corresponding to the recited mobile station and service network) (see, for example, col. 7, lines 15-25).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement a key usage counter as taught in Marshall in the method of Aura because it would provide a means for updating the encryption key (col. 2, lines 10-20) and that in turn would prevent an outsider to eventually gain access to the encryption keys (col. 6, lines 35-40).

Claim 28

Marshall discloses the use of a counter in association with the usage of an encryption key by each terminal (corresponding to the recited mobile station and visiting network) (see, for example, abstract; col. 7, lines 15-25).

Claim 29

Marshall discloses the use of counters in association with the usage of encryption keys by both terminals (corresponding to the recited mobile station and service network). When the counters reach a predetermined value (corresponding to the recited comparing the indicator of the service network with the indicator of the mobile station) a new key is transported to the terminal that corresponds to the recited transmitting information corresponding to the value to the station (see, for example, abstract; col. 7, lines 15-25).

Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Aura (6,711,400 B1) in view of Marshall et al (4,888,800; hereinafter Marshall) and further in view of Maupin (6,600,917 B1).

Claim 32

Aura discloses:

determining whether the home environment and the service network share a cryptographic primitive (see, for example, Fig. 3, where the home network at stage 302 uses the primitive TA11 for calculation of KS and the service network BS uses primitive TA12 at stage 312 to calculate DCK1 which also calculated by MS at stage 323 using TA12. The calculation of DCK1 at MS is dependent upon the value KS. This implies that the home network is aware of the primitives used at the BS and based on this knowledge the home network transmits the required authentication vector to the visiting network to be used by a specific primitive which corresponds to the recited determining whether the home environment and the service network...);

computing a shred secret key (SSK) (see, for example, Fig. 3, where the cryptographic key DCK is computed at the visiting network);

transmitting information from the service network to the station that enables the station to compute the SSK (see, for example, col. 7, lines 13-25; Fig. 3, stage 327).

Aura, however, does not expressly disclose that if it is determined that the home and visiting networks do not share a cryptographic primitive, the 3GPP AKA is used for authentication operation between the mobile station and the visiting network.

Maupin teaches a telecommunication system that a base station (corresponding to the recited service network) transmits a message to inform mobile units of the type of services supported by the base station (see, for example, abstract; col. 2, line 64-col. 3, line 12). Maupin further discloses that based on the message that is received from the base station a mobile unit decides on the use of an available technology such as 3GPP, which is capable of using it for communication with a base station (see, for example, col. 3, lines 21-47). This process corresponds to the recited determining whether to use a 3 GPP AKA technology or a shared cryptographic primitive between a home network and a service network, because a mobile unit only capable of using a technology that its home environment network uses.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the process of determining to use a 3GPP AKA technology or a shared cryptographic primitive as taught in Maupin in the system of Aura, because it would enable the mobile unites to quickly determine what type of technology is available to them (col. 2, lines 57-61).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US patent No. 6,463,055 B1 to Lupien et al.

US patent No. 5,915,021 to Herlin et al.

US patent No. 5,091,942 to Dent

US patent No. 5,940,512 to et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132

AN, a.n.

September 24, 2004

Gilbert S.
GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100